Security's Biggest: ISC East Expo, Aug. 28-30, New York City C1850-12

A CAHNERS PUBLICATION

AUGUST 1990

SECURITY™

THE MAGAZINE FOR SECURITY DECISION MAKERS

Tom Nagle
Director of Corporate Security and Administration
Levi Strauss & Co.

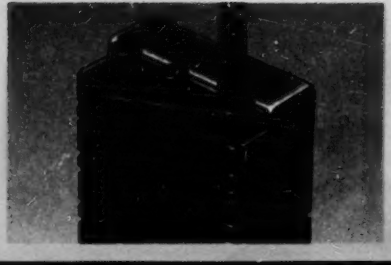
TAILORED PROTECTION p. 42

Improving Security Audits p. 36

Facilities Management Services p. 57

Innovative Guard Tour Systems p. 48

Equipment Focus: Portable Radios p. 62



SECURITY T.M.

THE MAGAZINE FOR SECURITY DECISION MAKERS

A CAHNERS PUBLICATION/VOLUME 27, NUMBER 8/AUGUST 1990

DEPARTMENTS

1 Express Request

11 Editorial/Masthead

12 Security Indicators
Security increases its reliance on equipment but not at the expense of personnel.

17 Idea Exchange
A Corporate Action Kit provides employee awareness training at minimal cost.

Incipient fire protection equipment protects a computer data center. (p. 17)

23 Strategies
Discover the secrets to getting approval for security projects.

27 Issues
A requirements document is an essential security management tool.

FEATURES

36 SECURITY SURVEY YIELDS RESULTS
Are you getting the most from security surveys? Planning, refinement and perseverance are crucial.

Security surveys offer evaluations and create a framework for action. (p. 36)

Cover Story

42 SECURITY'S COMFORTABLE FIT
Broad responsibilities help security adapt to a changing marketplace — and increase its necessity.

48 GUARD TOURS GO HI-TECH
Electronic guard tour systems measure officer efficiency and save supervisor time.

52 POLICIES, PROCEDURES, DEVICES LAG INFO SECURITY THREATS
Computer downtime causes financial loss at 50 percent of organizations. Is your company at risk?

55 INFO BRIEFS

On the Cover
Tom Nagle, director of corporate security and administration, contributes to the overall success of Levi Strauss & Co. by taking on broad responsibilities. (p. 42)

SERVICES

57 Facility Managers Assist Security

EQUIPMENT FOCUS

62 Security Takes Center Stage With Feature-Packed Portable Two-Way Radios

68 Product Update

More than 60 products, including this integrated security system, are featured this month. (p. 68)

86 Literature

87 Classified

89 Suppliers Index

90 Endpieces

91 Reader Service Cards

Cahners Publishing Company, A Division of Reed Publishing USA ☐ Specialized Business Magazines for Building & Construction ☐ Research ☐ Technology ☐ Electronics ☐ Computing ☐ Printing ☐ Publishing ☐ Health Care ☐ Foodservice ☐ Packaging ☐ ☐ Environmental Engineering ☐ Manufacturing ☐ Entertainment ☐ Home Furnishings ☐ and Interior Design. Specialized Consumer Magazines for Child Care ☐ Boating ☐ and Wedding Planning.

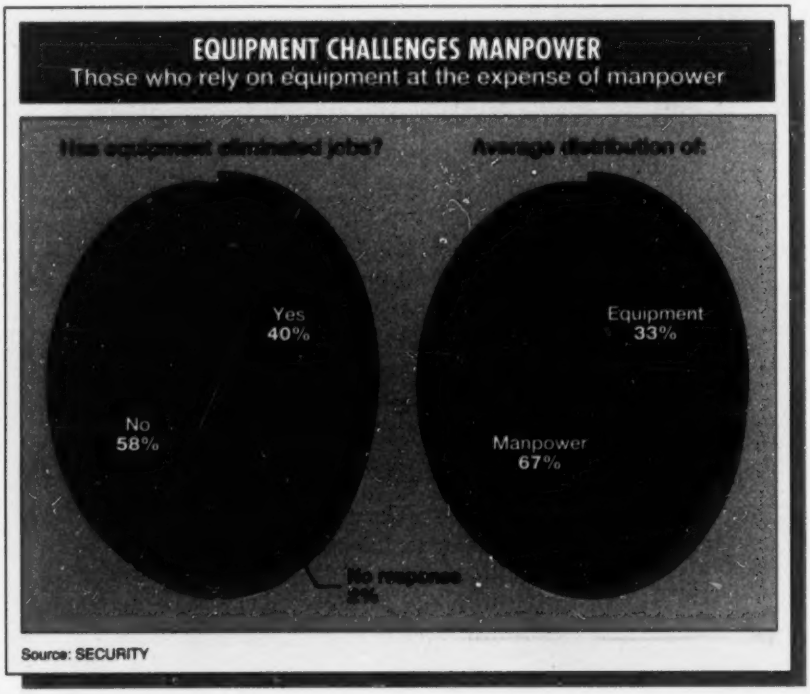
SECURITY (ISSN 0890-8826) is published monthly, except for March and August when two issues are published in national and separate editions, by The Cahners Publishing Company, A Division of Reed Publishing USA, 275 Washington St., Newton, MA 02158-1630. Terrence M. McDermott, President; Charles E. Moodhe, Senior Vice President/General Manager, Chicago Division; Jerry D. Neth, Senior Vice President/Publishing Operations; J.J. Walsh, Senior Vice President/Finance; Thomas J. Dellamaria, Senior Vice President/Production and Manufacturing; Ralph Knupp, Vice President/Human Resources. Circulation records are maintained at Cahners Publishing Company, 44 Cook St., Denver, CO 80206-5800. Phone: 303/388-4511. Second-class postage paid at Denver, CO 80206-5800 and additional mailing offices. Postmaster: send address corrections to *SECURITY* at 44 Cook St., Denver, CO 80206-5800.

SECURITY copyright 1990 by Reed Publishing USA; Ronald G. Segel, Chairman and Chief Executive Officer; Robert L. Krakoff, President and Chief Operating Officer; William M. Platt, Senior Vice President.

Annual subscription rates for non-qualified people: USA, $59.95; Canada/Mexico, $89.95; other countries, $115 for surface mail and $165 for air mail. Special issues, including product directory, are $50. Except for special issues where price changes are indicated, single copies of regular issues are available for $10, $14 and $18 (USA, Canada/Mexico and foreign). Please address all subscription mail to *SECURITY*, 44 Cook St., Denver, CO 80206-5800.

SECURITY INDICATORS

Trends and forecasts for determining loss prevention needs.



For the most part, security retains personnel despite mounting equipment purchases. Industrial security most likely increases reliance on equipment.

SECURITY SURVEY

Manpower Distribution Holds Its Own In Wake of Increased Equipment Reliance

It's in the headlines all the time: People lose their jobs when faster and more powerful technology enters the workplace. Within security departments, security technology has eliminated some jobs, says SECURITY's Second Quarterly Telephone Survey, but manpower continues to satisfy two-thirds of security's needs.

DATA SECURITY BANK

Less than half of survey respondents — 40 percent — say their department increased reliance on equipment at the expense of human resources in the last year. Industrial respondents are most likely to increase equipment reliance, at 62 percent. Institutions continue to depend on human resources to satisfy security needs; just 13 percent increased equipment reliance at the expense of personnel in the last year.

Manpower allocation dominates equipment use, the survey says. On the average, manpower distribution accounts for 67 percent of security resources. Retail reports the highest manpower dependence: 33 percent of retail respondents look to manpower to satisfy 90 to 99 percent of security's tasks. The government also reports steady manpower dependence: 50 percent of government respondents say manpower performs 70 to 79 percent of tasks.

Organizations that employ fewer than 500 people depend on human resources most often to get the job done, according to the survey.

SUBSTANCE ABUSE

Testing Status Affects Substance Abuse Perceptions

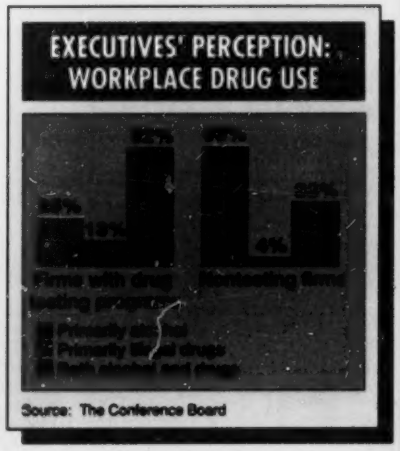
Firms engaged in drug testing are twice as likely as their nontesting counterparts to characterize their substance abuse problems as alcohol-and drug-related as opposed to exclusively alcohol-related. This according to a survey of 681 major corporations conducted by the Conference Board.

Companies that do not conduct drug tests are most concerned with problems related to alcohol abuse and addiction, the study says, while testing companies perceive both alcohol and drugs as workplace problems.

The decision to test employees for drugs usually requires input from several departments within an organization, the survey shows. On the average, executives from at least four areas determine drug abuse policy. The human resources department is involved 94 percent of the time; security is called on to help with the decision-making process 26 percent of the time.

The decision to test employees for drugs is most often reached following six to 11 months of consideration, the survey says.

Among the perceived benefits of drug testing, improved applicant quality and safer work environment top the list.



Nontesting firms perceive alcohol as the most abused substance.

EMPLOYEE THEFT

Weak Awareness Secures Sky-High Theft Figures

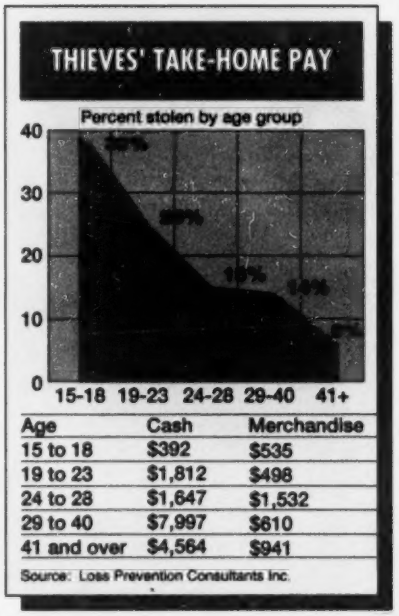
Opportunity — not job title or length of service — encourages employees to steal, says a Loss Prevention Consultants study titled "The Silent Partner — How Many Do You Have?" The study, which is based on thieves' confessions, documents theft activities among 345 employees responsible for $1,031,970 in shrinkage over a four-year period.

Employee theft is not a "seasonal virus" according to the study. On the average, the employees took cash or merchandise during more than 50 percent of days worked.

Accessibility — more than financial need — fuels thieves' desire to steal, the study finds. Among 15- to 18-year-olds, 50 percent say they stole because it was easy. Reason for stealing evolves with age, however; 52 percent of those 41 and over steal to satisfy financial needs. Younger thieves are more likely to steal electronics and gadgets, while older employees more often steal cash.

William Urban, president, Loss Prevention Consultants, Minneapolis, says heightened security awareness is the key to cutting down employee theft.

"Catching thieves early is crucial, because once they start stealing they don't stop until they're caught," Urban tells SECURITY. "Begin by informing employees about theft consequences during orientation. Don't just throw in a five minute discussion about theft at the end of orientation. Taking 20 minutes to explain the program and that it must be taken seriously saves time and money later."



Age	Cash	Merchandise
15 to 18	$392	$535
19 to 23	$1,812	$498
24 to 28	$1,647	$1,532
29 to 40	$7,997	$610
41 and over	$4,564	$941

Source: Loss Prevention Consultants Inc.

While younger employees steal most often, older groups steal more cash.

NEWS

Security Wrap-Up: Drug Testing, Homelessness

▶ The National Security Institute calculates that **employee drug testing** is a billion dollar a year industry. Employee dishonesty, however, costs American business $50 billion a year, the Institute says.

▶ When dealing with the current **homeless population** of 500,000, these demographics from the Manhattan Institute can better prepare security for confrontations. Between 80 and 90 percent of the homeless are men, but families make up 23 percent of the total homeless population. Among singles, 20 percent have been homeless for four years. Between 28 and 48 percent of the homeless are mentally ill, and at least one-third are substance abusers. Homeless individuals are likely to sleep in public places, while families seek city-provided shelters. At least 50 percent of the currently homeless have been homeless before.

▶ The Justice Department will award **anti-drug abuse grants** totaling more than $395 million to states and municipalities during 1990. Eligible states will receive at least $987,753, with more based on population size. Local governments will also receive grants.

PURCHASING

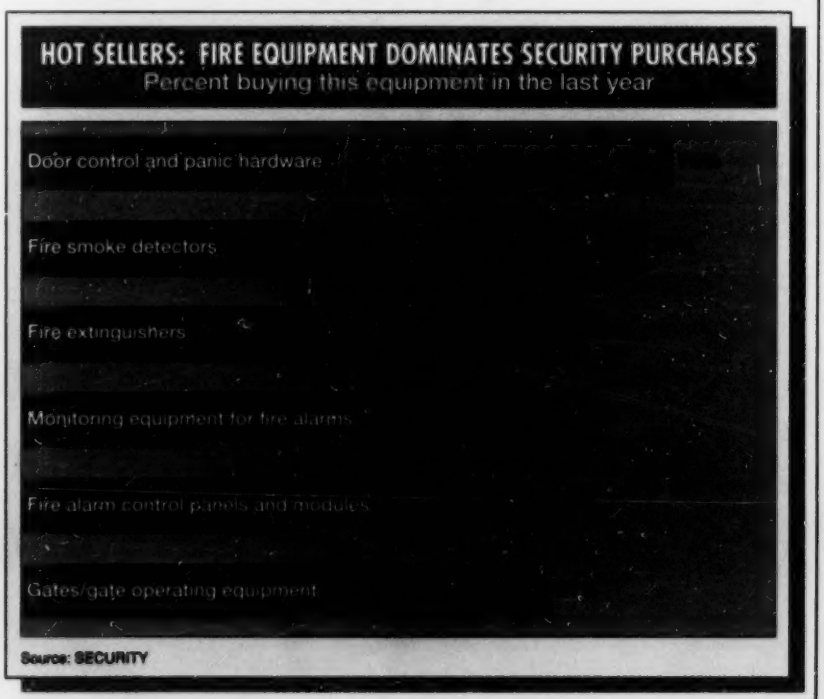
Door Control, Fire Equipment Attract Security Dollars

Fires are a hot concern among those who purchase security equipment, according to SECURITY's Second Quarterly Telephone Survey of security decision makers.

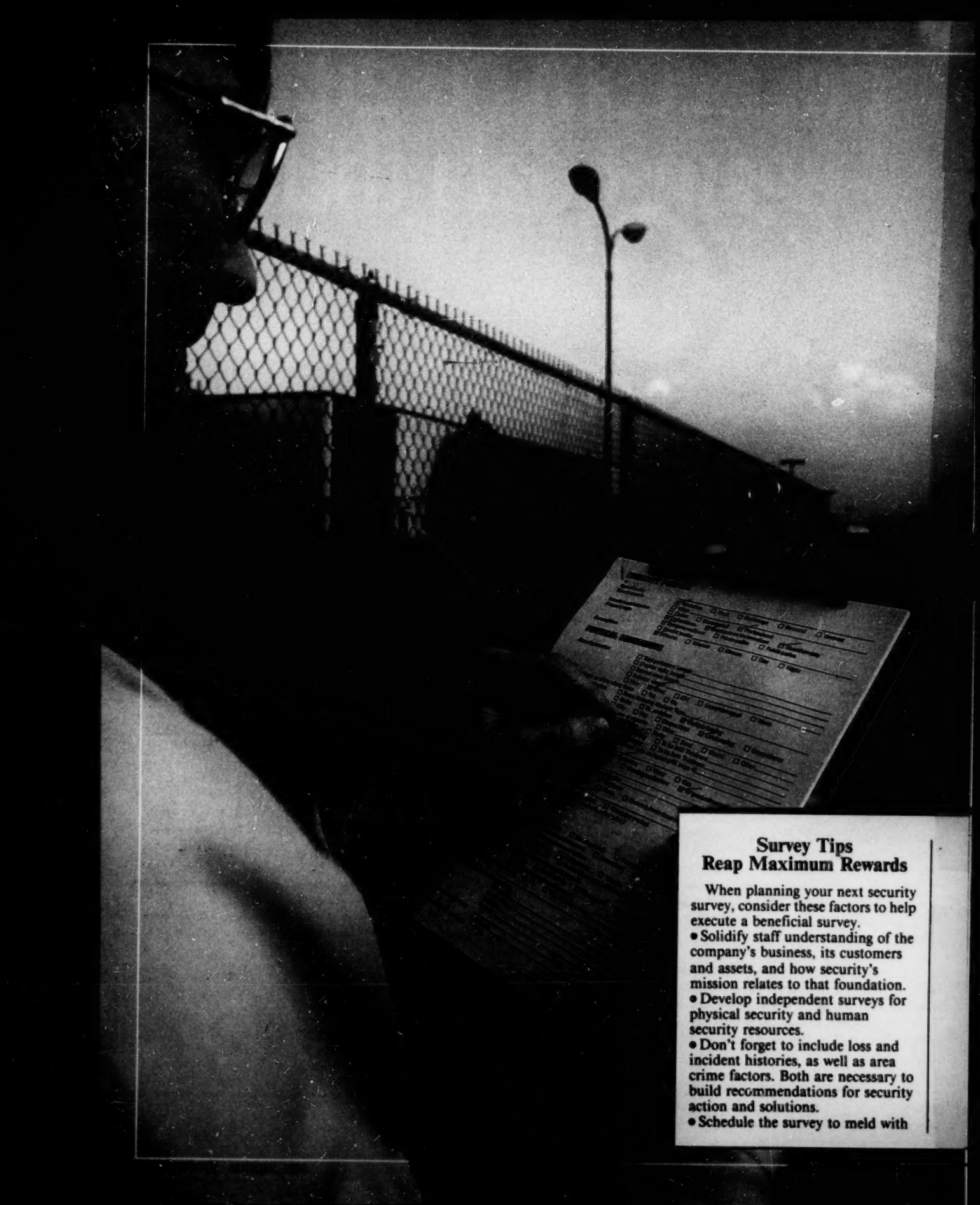
While door control and panic hardware were most frequently purchased by respondents in the last year, fire-related equipment falls into the next four slots for popularity.

Big sellers specific to type of business were fire smoke detectors, which 81 percent of industrial respondents and 75 percent of retail purchased; fire extinguishers, which 83 percent of retail purchased; gates and gate operating equipment, which 72 percent of industrial and government respondents purchased; and door control and panic hardware, which attracted 81 percent of industrial and 75 percent of retail respondents.

Turnstiles, guardrails and grilles scored low among all groups of prospective buyers.


HOT SELLERS: FIRE EQUIPMENT DOMINATES SECURITY PURCHASES
Percent buying this equipment in the last year
Door control and panic hardware
Fire smoke detectors
Fire extinguishers
Monitoring equipment for fire alarms
Fire alarm control panels and modules
Gates/gate operating equipment
Source: SECURITY

Fire equipment dominates the list of best-selling security equipment. Retail buyers were especially active in acquiring new fire-related equipment.



Survey Tips Reap Maximum Rewards

When planning your next security survey, consider these factors to help execute a beneficial survey.

- Solidify staff understanding of the company's business, its customers and assets, and how security's mission relates to that foundation.
- Develop independent surveys for physical security and human security resources.
- Don't forget to include loss and incident histories, as well as area crime factors. Both are necessary to build recommendations for security action and solutions.
- Schedule the survey to meld with

SECURITY SURVEY YIELDS RESULTS

The tried and true security survey does more than identify assets, vulnerabilities and solutions — it's a bona fide management tool.

By Rebecca D. Russell
Senior Editor

The mirror doesn't lie; neither do security surveys.

A thorough security survey provides the good and not so good truths about security's accomplishments. It's a seasoned tool that pinpoints areas for improvement, whether checking perimeter controls or determining manpower effectiveness.

Getting the most from a security survey takes initiative, planning and requires perseverance.

Whether checking perimeter controls or manpower effectiveness, the security survey offers evaluation, creating a framework for action.

The ever-changing face of business provides incentive to keeping surveys up-to-date. Restructurings, acquisitions and mergers often force the issue: A new boss or potential purchaser may request a survey to better understand what threats and protections exist.

Change Provides Opportunity

"Many corporations don't realize security is intangible. They accept losses up front, then pass the cost on to consumers. It does affect the bottom line," says Richard Haynes, a Charleston, W. Va.-based consultant.

Harold Rudd, security supervisor, Cincinnati Milacron, says a recent buyout and management shift at the Maineville, Ohio, company gave security the opportunity to conduct its first formal survey in five years.

"I walked around the building last week and saw problems. One fence is overgrown — it's something that has been let go. I'd like to get it cleared, but we've had financial and personnel problems recently, just like a lot of other businesses," he says.

Work site changes signal that it's time for security to take a fresh look, says Ray Chambers, CPP, president, Assets Protection Systems Associates Inc., Largo, Fla. Changes can include a building addition, equipment retrofit, staff growth or cutback, lighting revamp or office space reconfiguration. Changes to company or neighbor perimeter also need addressing.

In fact, Chambers says, a survey may point out changes that security didn't know about — also providing a good time to reiterate security's capabilities and need to know.

Another bonus: security may discover that it would make fiscal sense to share tasks/responsibility with other departments. A recent SECURITY survey found that 54 percent of respondents share some costs with another department. Of those that share, 54 percent do so to reduce operating costs, 23 percent to consolidate departments.

Frequency Reflects Philosophy

How frequently your security department surveys operations depends on the industry and business philosophy toward security itself.

SECURITY's recent national telephone survey discovered that 71 percent of security decision makers say their department conducts security audits/surveys.

That study also shows survey frequency (see chart, "Frequency Reflects Philosphy"). The largest percent of respondents, 24 percent, conduct a survey twice a year, while 23 percent survey annually. On the opposite end of the spectrum, 9 percent survey weekly while 6 percent say the survey is an ongoing, continuous task.

Sharon Lutz, director of security, Breckenridge Frontenac Hotel, says surveys are an ongoing responsibility for the St. Louis hotel's 10-member security staff.

"The staff doesn't mind doing it because we take a lot of pride in our work. We realize that potential loss could kill us," she says.

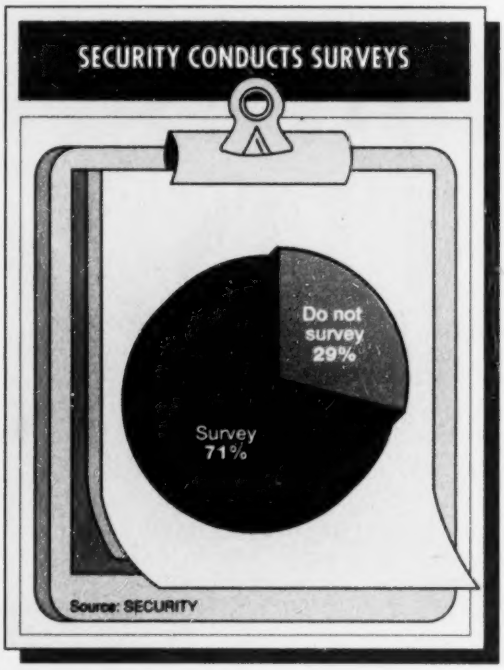
Once each week, an officer conducts a formal fire and safety equipment inspection, including a written report.

Frank Gonzalez tailor-made a security survey for new construction pro-

fiscal planning. Findings may prompt requests for additional funds and/or cost and manpower sharing with another department.

- Talk with managers and employees to learn their needs. After the survey, keep staff and employees up to speed on meeting challenges and maintaining security.
- Work with a consultant to gain a fresh perspective at familiar sites.
- Make sure employees keep security abreast of changes in the workplace.
- Wrangle senior management understanding of this project. Share recommendations and security action to show how the department meets vulnerabilities.

Up-to-Date Surveys Translate to Bottom Line Terms



The majority of security decision makers survey physical protection and/or manpower.

jects. As Liz Claiborne's director of corporate security in North Bergen, N.J., Gonzalez heads security for multiple sites and new construction: 10 distribution centers, two office buildings, two soon-to-be-constructed office buildings, plus 80 existing retail stores and 12 new stores under construction this year.

Gonzalez uses a three-stage survey for each new site. Before each survey he addresses these points.

- Consider the business, its goals and objectives.
- Pre-planning is essential. "You can't expect to go in there and wing it," he says.
- Talk with building occupants and learn their needs. With so many new construction projects, this is a necessity for Gonzalez. One new facility will house a check-generating payroll area; future occupants expressed the need for extra precautions in this area and security's construction plans reflected that need.

Squeezing Time for a Survey

This communication link is crucial to survey success. When refining or planning a survey, talk with organization decision makers to ensure a match between the areas that can be surveyed, what all parties can expect as a realistic response and how the survey can impact the company.

Like a growing number of security decision makers, Charles Baron-Klask hires a consultant to conduct an annual survey. It saves staff time and provides crucial certification that affects business profit.

Baron-Klask is chief of security at Technicolor Videocassette of Michigan Inc., Livonia. Membership in the Motion Picture Association of America Inc. includes access to that body's security consultant.

"When we go around our site on our own, we are more apt to overlook things," he says. "The consultant will tell you things you don't necessarily want to hear."

Sign Up for Survey

Once a year he schedules a general time for the survey; he learns of the actual date 24 hours beforehand. The surveyor discusses findings and recommendations using a 20-page form. He says security follows through on recommendations as budget permits.

Conducting this annual survey translates directly to business terms because Technicolor is one of the leading videotape reproduction houses in the country, serving major film studios. "That our security passes the test directly relates to the amount of business we get; these studios will only work with people approved by MPAA," Baron-Klask says.

Like Baron-Klask, Lutz sees direct results from security's surveys — in the form of insurance cost breaks. When weekly surveys indicated vulnerabili-

Resources Soothe Survey Woes

Publications and services provide guidance in producing a survey. Here are some true blues and new kids on the block. Circle the corresponding number on the reader service card for complete information.

- *Protection of Assets Manual and Bulletin* includes a four-volume manual plus monthly updates with practical management information. Circle 160
- *Introduction to Security and Loss Control*, by Norman R. Bottom Jr., CPP, and John Kostanoski, published by Prentice Hall. Includes a chapter on loss control surveys. Circle 161

Personal and Organizational Security Handbook, second edition, by S. Blumenkrantz, published by Government Data Publications. Includes a workbook. Circle 162

Security: Adequate or Not? by Chris E. McGoey, CPP, published by Aegis Books. Examines premises liability litigation and security evaluation. Circle 163

- The CAP Index was developed by Robert Figlio, Ph.D., to help businesses assess crime vulnerability. Circle 164
- "Retail Shrinkage Control Questionnaire" helps those in the retail sector identify control loopholes. Mention SECURITY and it's free for the asking at Coopers & Lybrand, Attn.: Publications Dept., 1251 Avenue of the Americas, New York, N.Y. 10020 or phone (212) 536-3257. Circle 165

ties, security added safety programs in response. "That is bringing our premiums down," she says.

"We notify our carrier any time we do something new. They monitor it to see how it is going," she says. Establishing a safety committee and fire management both helped; other programs have reduced the premium on worker compensation insurance, she says.

Fine-Tuning for Maximum Results

It's critical to include crime analysis information says Scott D. Roulston, CPP, president of Topwatch Corp., Cleveland.

When refining and planning a survey, talk with organization decision makers to ensure a match between objectives and results.

Norman Schroeder, director of security, Hoffmann-LaRoche & Co., Nutley, N.J., includes the CAP Index in site evaluation. The index helps business determine a neighborhood's vulnerability and foreseeability of crime — hot topics in litigation.

"The specificity and refined data of the survey appealed to management. We pursuaded them to include it when new sites are being built," Schroeder says.

"Sometimes the results are almost incredible. We see a facility in what you would think is a sleepy little town and the results say otherwise," he says. Then, it takes work to "sell" the credibility of the study.

There are innumerable tools to help get the maximum output from security input (see "Resources Soothe Survey Woes"). Just as decision makers customize surveys to meet business needs, others fine-tune their tools to maximize results.

Tom Woodal, director of the Physical Security Division of General Services Administration's Federal Protective Service, Washington, D.C., developed a tool now used by more than 7,000 sites nationwide. The computer-based Risk Assessment Matrix (RAM) provides a list of potential risks as well as recommended countermeasures, costs and scheduling information.

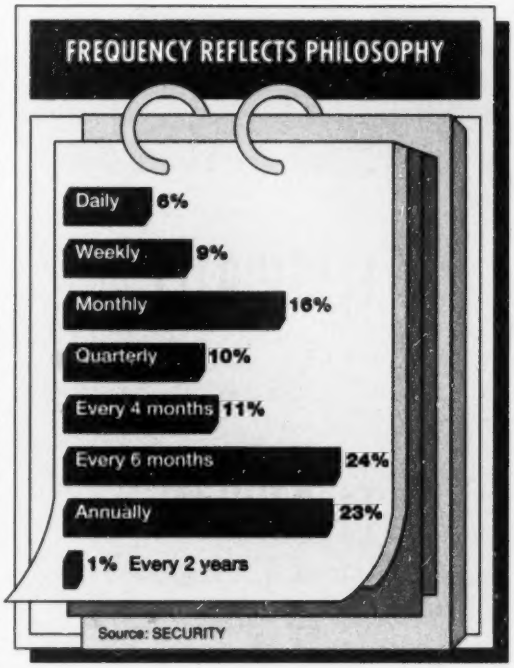
This information is compiled when combined with the results of a manual physical security survey. RAM then examines 10 attributes which affect security. Results also incorporate crime incidents in or around the building in the last year.

Communicate for Success

Don't forget the human element when looking to maximize return on survey investment. Once the results are in, it's important to keep communicating with staff members and participants outside the department. That will better facilitate full participation, to maintain successful levels of security and accomplish new goals.

At this stage, planning and foresight pay off. If security has taken the time to build management interest in the exercise plus seen to it that realistic goals can be accomplished, the survey will prove to be time well spent.

It requires management support, Haynes says. "You have to feel your industry and what management wants," he says. "A survey helps you identify strengths, weaknesses and vulnerabilities. Yet often after it is done it gets put on a shelf. It all begins and ends with management and their attention to security." □



Survey frequency varies according to company philosophy, industry, staff capability and resources.

The Survey As Security Awareness Tool

By expanding the definition of a security survey, you can measure security awareness and perception among employees.

Consultant Richard Haynes recommends regular awareness surveys. Ask: " 'Do you educate your employees on the importance of security?' " he says. "Employees must be able to identify the significance of their participation. If they can see specific threats, they will be more inclined to help with security efforts."

Employee surveys are gaining popularity. It can be as simple as a questionnaire distributed to employees, asking key questions related to security operations and services. In return you can identify strongpoints and see any perception problems.

Also consider a survey of company hiring and screening practices, suggests consultant Ray Chambers. By looking at the process, from interviews to background checks, security can learn what will improve the process to enhance security efforts.

Policies, Procedures, Devices Lag Info Security Threats

Networking, lack of planning put computers at risk, says national info security study.

By Bill Zalud
Editor

More than four out of every 10 U.S. businesses may be unnecessarily vulnerable to breakdowns that stop the flow of critical information, according to the 1989 national Ernst & Young Computer Security Survey.

The survey gauges opinions of upper-level management, security and data processing management, and analysts and auditors.

Not surprisingly, computer system failures or downtime caused financial losses at 50 percent of organizations in the past two years. At the same time, about 23 percent reported financial losses because of malicious acts.

Getting a handle on the dollar extent of damage indicates most losses congregate at the lower end. Dollar figures remain the same or decrease slightly when compared to Ernst & Young's 1988 survey. For example, of the 23 percent reporting malicious act losses, 16 percent lost up to $50,000, due to acts including fraud and embezzlement. It was 18 percent the year previous.

Further, 5 percent experienced $50,000 to $1,000,000 in losses and 2 percent had losses of more than $1,000,000.

Yet, respondents are — as a group — convinced that information and computer security is important and security risks are increasing.

Risks Increase

While 84 percent believe information and computer security is important, 71 percent report risks increased over the past five years, a 21 percent increase over the year before.

Most respondents also believe risks

INFO SECURITY GOALS: MANAGEMENT VS. SECURITY

Security	Where Invested	Management
42 percent	System Availability Continuity	59 percent
19 percent	Data Confidentiality	7 percent
27 percent	Data Integrity	20 percent
12 percent	Business Continuity	13 percent

Source: Ernst & Young

Management stresses use of computers while security stresses protection needs.

TYPES OF PROTECTION

Percent Using	Solution
82 percent	Optional access control software — ACF2 and RACF, for example.
73 percent	Uninterruptible power sources (UPS).
63 percent	Redundant communications or power to avoid single points of failure.
28 percent	Virus detection software — relatively inexpensive and limited protection.
20 percent	One-time, token-based passwords.
18 percent	File encryption.
14 percent	Communications encryption.
11 percent	Encryption-based personal computer access control.

Source: Ernst & Young

Shared and embedded schemes and quick fixes are most attractive types of protection.

are increasing on pace or even faster than the growth of computing in their organizations.

Driving the risks up: organized, sophisticated perpetrators; increased dependence on computers to conduct business; and growth of networking. Networking brings computer access to more people and allows sharing of applications and data bases inside and outside organizations.

The source of threats also shifts. Last year respondents felt threats came more from inside than outside. For instance, 44 percent are most concerned with protecting information from employees who do not need to know, while 32 percent cite the need to protect information most from competitors.

The year before, competitors beat out employees as the number one threat. The difference: manufacturing companies see competitive threats more keenly than service organizations. And, as the economic balance tips to services, a traditional perspective will diminish.

Differences in Viewpoint

Security and upper management split when it comes to where to invest security resources.

While both see computer service availability and continuation as the essential first area to protect, security seems more committed to the issues of confidentiality and integrity.

Yet, if continuity is of prime importance, there's too little planning for it. Only 16 percent of firms report formal, written business continuity plans, including testing with appropriate drills, walk-throughs and third-party reviews.

Access Weaknesses

Access control is another tool inconsistently applied. A vast majority of firms (87 percent) limit data center access to people who work in it. But 13 percent permit access by other data processing personnel, whether they work in the center or not.

Controlling data access also is spotty. On the one hand, 54 percent restrict data access to authorized personnel and limit users to only data required for their jobs. On the other hand, 30 percent limit data access control to computer-resident data only.

More risky yet, 16 percent either have no access control program or permit users access to all data except as otherwise restricted.

Protection Devices Vary

There's a diversity of security technologies and products to protect equipment, software and data.

Not using available technology is a minor irritation compared to the damage that a lack of policies can cause. Yet, nearly two out of 10 organizations have no policy or policy requirements specific to their information assets. □

More Planning; Cover Real Threats

Among major conclusions of the Ernst & Young Survey:

- Not enough planning.
- Only 16 percent of companies acknowledge thorough, organization-wide business continuity planning, despite strong emphasis on integrity and availability as key objectives.
- With encryption already available, only 5 percent use it for all confidential data in public networks.
- As computers network and share data bases and applications, only 17 percent say unintended use of networks is an important issue.

When defining network threats, 38 percent of organizations answering the survey say tampering or interference with the intended operation of the network or the unintended use of the network are prime security concerns. Threats to computer applications from users of the network was mentioned by 26 percent of respondents.

The loosey-goosey nature of emerging networks makes things tougher: 10 percent are unable to safely identify network users.

TYPES OF POLICIES

Percent Having	Policy Type
71 percent	Policies state who controls data access.
53 percent	Require informing all employees of their data security responsibilities.
32 percent	Data security orientation for new employees.
28 percent	All data labeled — sensitivity to disclosure.
26 percent	Data security responsibility separate from continuity of service and business.
17 percent	No policy requirements.

Source: Ernst & Young

Data ownership is popular, while nearly two out of 10 have no policy requirements.

SOURCE OF THREATS: MANUFACTURING VS. SERVICE COMPANIES

Manufacturing	Source of Threat	Service
39 percent	Employees	48 percent
38 percent	Competitors	28 percent

Source: Ernst & Young

Manufacturers traditionally see competitors more as a security threat.